

## UNITED STATES DISTRICT COURT

for the

WESTERN

DISTRICT OF

OKLAHOMA JUL 28 2017

FILED

CARMELITA REEDER SHINN, CLERK  
U.S. DIST. COURT, WESTERN DIST. OKLA.  
BY ASB DEPUTYCase No: M-17-349-SM

In the Matter of the Search of )  
 (Briefly describe the property to be search )  
 Or identify the person by name and address) )  
 PROPERTY KNOWN AS )  
 User name: **Robert Apgar** and/or )  
 Account name: **icecreamman0032@gmail.com** )  
 IN THE POSSESSION OF: )  
 Wildec LLC )  
 Meet24.com Social Networking Application )  
 2525 Ponce De Leon Blvd., #1250 )  
 Coral Gables, FL 33134 )

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property (*identify the person or describe property to be searched and give its location*):

See Attachment A, which is attached and incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section*

*Offense Description*

18 U.S.C. § 2251(a) and (e)  
 18 U.S.C. § 2252(a)(1)  
 and  
 18 U.S.C. § 2252(a)(4)(B)

Attempted sexual exploitation of children;  
 Transportation of child pornography;  
 Possession of child pornography.

The application is based on these facts:

See attached Affidavit of Special Agent Charles Stanley, Federal Bureau of Investigation, which is incorporated by reference herein.

☐ Continued on the attached sheet(s).

☐ Delayed notice of \_\_\_\_\_ days (*give exact ending date if more than 30 days*) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).



*Applicant's signature*

CHARLES STANLEY  
Special Agent  
Federal Bureau of Investigation

Sworn to before me and signed in my presence.

Date: 7-28-17



*Judge's signature*

City and State: Oklahoma City, Oklahoma

SUZANNE MITCHELL, U.S. Magistrate Judge  
*Printed name and title*

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, Charles Stanley, being duly sworn, state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), in Oklahoma City, Oklahoma. I have been employed as a Special Agent since May 2016.

**PURPOSE OF AFFIDAVIT**

2. This affidavit is made in support of an application for a search warrant to search for and seize instrumentalities, fruits and evidence of violations of 18, U.S.C. §§ 2251(a), 2251(e), 2252(a)(1), and 2252(a)(4)(B). These items are more specifically described in Attachment B.

3. This affidavit is submitted in support of an application for a search warrant for the contents of **Robert Apgar's Meet24 account**, further described in Attachment A.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information made available to me by other law enforcement professionals. These facts are provided for the sole purpose of establishing probable cause for the issuance of the requested search warrants; therefore, this affidavit does not necessarily contain all information uncovered during this investigation.

**JURISDICTION**

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a),

(b)(1)(A) & (c)(1)(A). Specifically, the Court [is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

6. Robert Apgar has been identified through this investigation to be involved in attempted sexual exploitation of children, transportation of child pornography, and possessing or accessing child pornography.

7. A federal search warrant was executed on December 8, 2015, at the Patricia Jaques residence at 4204 Southeast 49<sup>th</sup> Street, Oklahoma City, Oklahoma. (Jaques was Robert Apgar’s mother.) Robert Apgar was present. Agents seized several computers (including smartphones and a laptop) (the “DEVICES”) and transported them to the FBI/Oklahoma City Evidence Control Room. During an interview of Robert Apgar at the residence, he told agents that he used his mother’s wireless network to access the Internet.

8. FBI computer forensic analysts processed the DEVICES, and made the images they contained available to SA Joshua Payne in a consolidated format for his investigative review. During his review of the DEVICES’s content, SA Payne saw multiple images of what appeared to be prepubescent females in sexually provocative positions. The images ranged from partially clothed to fully nude females. SA Payne could see the prepubescent girls’ genitals in some of these sexually provocative images. Upon seeing what SA Payne believed to be child pornography, SA Payne stopped his review of the DEVICES and SA Payne applied for a second search warrant to specifically search for evidence of possession of child pornography. SA Payne stopped reviewing the DEVICES until such time a federal search warrant could be obtained to search the devices for violations of 18 U.S.C. § 2252A(a)(5)(B).

9. On November 4, 2016, Apgar was convicted for an Oklahoma state drug offense. He was sentenced to six years' imprisonment, and he is currently in state custody.

10. On February 11, 2016, SA Payne got a federal search warrant to search the devices for violations of 18 U.S.C. § 2252A(a)(5)(B).

11. Pursuant to that search warrant, I have reviewed some of the images captured by FBI computer forensic analysts from the DEVICES. On the laptop of Apgar's mother (which she said she allowed him to use in her home) is evidence that Skype was installed and that Skype user rapgar32 used Skype media messaging to transport child pornography pictures depicting prepubescent girls and attempt to sexually exploit children on October 19, 2015, and to possess such images on October 22, 2015, and October 29, 2015.

12. According to FBI forensic analysis, on October 19, 2015, Skype user jess13892 exchanged messages with rapgar32. At the beginning of the exchange jess13892 stated "hi its jessie from meet24."<sup>1</sup> During this Skype messenger chat, jess13892 indicated that she was 13 years old. At the beginning of the chat, Skype user rapgar32 said, "if u wanna do this ill [sic] go ahead and send the pics and vids that wa[y] u have them already." The user rapgar32 proceeded to send (via Skype messenger) jess13892 child pornography pictures as well as apparent child erotica. He attempted to send her videos, which he claimed were also child pornography. The user jess13892 asked who one of the girls depicted in a picture was, and rapgar32 replied, "tbh [to be honest] there [sic] just random girls that ive [sic] talked [to] and a lot of [them] just sent the pics with out me asking." Then rapgar32 added, "I never forced none of them it was all at there [sic] own choice just like I told u no

---

<sup>1</sup> Meet24 is an Internet-based cell phone app whose website says the app will help users: "Find singles nearby," "A lot of guys and girls online," and "Exchange messages and photos." Meet24 says users must be at least 13.

pressure.” The user rapgar32 then proceeded to discuss sexual activity with jess13892. At one point, he asked for a picture of her face. At one point rapgar32 said, “if we do meet face to face ill [sic] never make u do nuttin [sic] u don’t want to.” Towards the end of message exchange, rapgar32 told jess13892 that he drove a truck and delivered water for a living. I have since learned that at the time of the chat, Robert Apgar (who was 32 at the time the rapgar32 Skype account was created) delivered drinking water for a living. It thus appears that rapgar32 and jess13982 met on Meet24, discussed some kind of proposed interaction/exchange, then moved over to Skype messenger to continue their conversation and interactions. I am seeking this warrant to get content and information from Meet24 that sheds light on rapgar32’s initial interactions with jess13982—before he started sending her child pornography and child erotica via the Internet-based Skype messenger. I believe there is probable cause to believe that such content and information will constitute fruits, evidence, and instrumentalities of the foregoing violations.

13. Apgar’s Samsung Galaxy S5 phone was forensically examined. From that exam, I learned that the Meet24 application was installed on the phone. The Meet24 account utilized a Facebook one-click sign-on with the username being **icecreamman0032@gmail.com**. Thus, I am seeking a search warrant for the Meet24 account associated with the user name **icecreamman0032@gmail.com**. Open source research revealed that the same user name, **icecreamman0032@gmail.com**, is registered to the Facebook account of Robert Apgar. The Facebook account contains multiple pictures of Robert Apgar.

#### **BACKGROUND CONCERNING E-MAIL and REMOTE STORAGE**

14. In my training and experience, social media providers generally ask their subscribers to provide certain personal identifying information when registering for to use and application. Such information can include the user’s full name, physical

address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

15. In my training and experience, social media providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the social media application.

16. In my training and experience, in some cases, e-mail account users will communicate directly with application providers about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Application providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

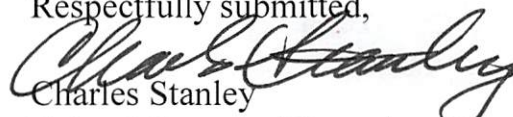
17. I know that social media providers such as Facebook and Kik store users' messenger chats, which can often be obtained through a search warrant. Thus, I believe Meet24 will have a record of Apgar's chats with Jessie / jess13892.

### CONCLUSION


18. Based on the aforementioned information, your affiant respectfully submits that there is probable cause to believe that Robert Apgar used a Meet24 account further described in Attachment A, to facilitate the foregoing violations and that fruits, evidence, and instrumentalities of such violations will be located in Apgar's Meet24 described in Attachment A.

19. Based on the forgoing, I request that the Court issue the proposed search warrant. The warrant will be served on Wildec, LLC, the owner and creator of Meet24 Social Networking application, who will then compile the requested records at a time convenient to it. Because the provider will compile the information requested in Attachment B at a time that is convenient to the provider, your affiant requests the warrant to be executed at any time of the day or night.

Respectfully submitted,

  
Charles Stanley  
Federal Bureau of Investigation

Subscribed and sworn to before me  
on the 28th day of July, 2017

  
\_\_\_\_\_  
SUZANNE MITCHELL  
United States Magistrate Judge



**ATTACHMENT A: Meet24**

**Property to Be Searched**

This warrant applies to information and content associated with user Robert Apgar and/or user name/account icecreamman0032@gmail.com that is stored at premises controlled by Wildec LLC Meet24.com Social Networking Application a company that accepts service of legal process at:

2525 Ponce De Leon, Blvd., #1250, Coral Gables, Florida 33134

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information and content to be disclosed by the Provider**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, chats, images, movies or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

1. The contents of all chats or communication between subscribers associated with the account, including stored or preserved copies of chats or communications sent to and from the account, draft chats or communications, the source and destination addresses associated with each chats or communications, the date and time at which each chats or communications was sent, and the size and length of each chats or communications;

2. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative

e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

3. The types of service utilized;

4. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, pictures, and files;

5. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

## **II. Information to be seized by the government**

All information and content described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. §§ 2251(a), 2251(e), 2252(a)(1), and 2252(a)(4)(B), occurring between October 1, 2015 and the present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- communications in any format with Jessie or jess13892 or Jess;
- communications with others regarding child pornography;
- child pornography;
- Information in any format relating to who created, used, or communicated with the account, including records about their identities and whereabouts.